ПРОБЛЕМЫ КИБЕРЗАЩИТЫ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

В.Н. Корделюк

Тенденции цифровой трансформации общества (в том числе в Республике Беларусь) показывают все большее внедрение автоматизированных, автоматических систем, реализующих сетевые информационные технологии по управлению технологическими процессами. Интернет был и остается основным каналом возможного воздействия на указанные системы в связи с все большим сопряжением технологических сетей и корпоративных информационных сетей.

Повсеместное функционирование объектов вооруженных сил, промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость национальную безопасность в различных сферах жизнедеятельности от их надежности и защищенности. При этом вскрывается пропорциональная зависимость – чем глубже интеграция автоматизированных систем управления в киберпространство, тем критичнее для данных объектов результаты активного воздействия извне на их информационные ресурсы [1].

В отличие от информационных сетей, где последствия реализации угроз (утечка информации, блокирование информации, ее несанкционированное уничтожение) имеют больше нематериальный характер, ущерб в сфере управления технологическими процессами в большинстве своем имеет непосредственную физическую форму (отключение электроэнергии, прекращение подачи воды, срыв работы телекоммуникационных сетей, аварии на железнодорожном, авиационном транспорте и т.д.).

Действия в киберпространстве позволяют наносить ущерб дистанционно (анонимно), не нарушая физических границ его государства. Возрастает важность кибербезопасности критически важных объектов инфраструктуры государства.

Список литературы

1. Концепция информационной безопасности Республики Беларусь: утв. Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1.

ЗАЩИТА УДАЛЕННОЙ ПОЛЬЗОВАТЕЛЬСКОЙ СТАТИСТИКИ С ПОМОЩЬЮ МЕХАНИЗМОВ ДИФФЕРЕНЦИАЛЬНОЙ ПРИВАТНОСТИ

Е.А. Криштопова

Автоматический сбор данных с пользовательских устройств (персональных компьютеров, смартфонов, фитнес-браслетов и т.п.) дает возможность сборщикам собрать информацию о конкретном пользователе – его предпочтениях, привычках, состоянии здоровья, режиме дня и т.д.

Например, для «анонимизированного» статистики просмотров пользователями фильмов компании Netflix, исследователи показали, что информацию о конкретных пользователях можно восстановить и предсказать их политические взгляды [1].

Вышесказанное делает важным задачу анонимизации пользовательской статистики. Технически это решается использованием механизмов дифференциальной приватности.

Дифференциальная приватность (Differential privacy - DP) – это совокупность методов, которые обеспечивают максимально точные запросы в статистическую базу данных при одновременной минимизации возможности идентификации отдельных записей в ней. Дифференциальная приватность дает математическое определение потери конфиденциальных данных отдельных лиц, путем внесения случайности, описываемой переменной ε, когда их личная информация используется для создания продукта.

Наиболее известны практические реализации локальных дифференциально-приватных алгоритмов: RAPPOR от Google, решения Apple для iOS 10, Microsoft’s PINQ, Uber’s FLEX.

Что касается белорусских производителей, то, так как деанонимизация пользовательской статистики не является требованием белорусского законодательства, то и алгоритмы дифференциальной приватности и аналогичные средства ими не применяются.

Список литературы

1. Narayanan, A., Shmatikov V. Robust De-anonymization of Large Sparse Datasets // 2008 IEEE Symposium on Security and Privacy (sp 2008). URL: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (дата обращения: 03.05.2019).

ПРЕПОДАВАНИЕ ДИСЦИПЛИН В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ СПЕЦИАЛЬНОСТЕЙ ПЕРВОЙ И ВТОРОЙ СТУПЕНЕЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Е.А. Криштопова, В.С. Осипович, А.М. Прудник

В настоящее время, вопросам информационной безопасности в Республике Беларусь придается очень большое значение [1, 2], кроме того, одним из государственных приоритетов нашей страны провозглашена ориентация на информационное общество и развитие рынка инфокоммуникационных технологий [3, 4].

Исходя из этого, для высших учебных заведений одной из актуальных проблем является подготовка специалистов как в области безопасности информационных технологий, так и в смежных областях с соответствующими компетенциями.

В свете стоящих задач, на кафедре инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» начато преподавание ряда дисциплин в области безопасности информационных технологий.

На 1-й ступени высшего образования по специальности 1-58 01 01 «Инженерно-психологическое обеспечение информационных технологий» преподается дисциплина «Криптографические технологии», в рамках которой изучаются базовые принципы криптографии, современные криптографические протоколы, студенты овладевают навыками применения криптографических технологий для защиты информации. На данную дисциплину для студентов дневной формы обучения отводится 32 академических часа лекций и 32 академических часа практических занятий.

Для студентов 2-й ступени высшего образования по специальности 1-59 81 01 «Управление безопасностью производственных процессов» преподается дисциплина «Безопасность информационных систем». Целью изучения дисциплины является получение знаний по вопросам обеспечения безопасности информационных систем в условиях различных по виду, происхождению и характеру возникновения угроз. На данную дисциплину для студентов дневной формы обучения отводится 10 академических часов лекций и 20 академических часов практических занятий.

Таким образом, внедрение кафедрой инженерной психологии и эргономики актуальных учебных дисциплин в области безопасности информационных технологий способствует решению задач качественной подготовки инженерных кадров в соответствии с вызовами времени.

Список литературы

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». URL:http://etalonline.by/document/?regnum=h10800455&q_id=754382 (дата обращения 02. 05.2019).

2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». URL:http://etalonline.by/document/?regnum=p219s0001&q_id=754197 (дата обращения 02. 05.2019).

3. Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы / Постановление коллегии Министерства связи и информатизации Республики Беларусь от 30.09.2015 г. № 35. URL: http://etalonline.by/document/?regnum=u215e2913&q_id=754159 (дата обращения 02. 05.2019).